Національний технічний університет України

«Київський політехнічний інститут ім. Ігоря Сікорського»

Кафедра цифрових технологій в енергетиці

ЗВІТ   
з виконання лабораторної роботи №3  
з дисципліни «Безпека інформаційних систем»

«**Шифр Гамування**»

Виконав: студент групи ТР-12 Каркушевський В.Л.

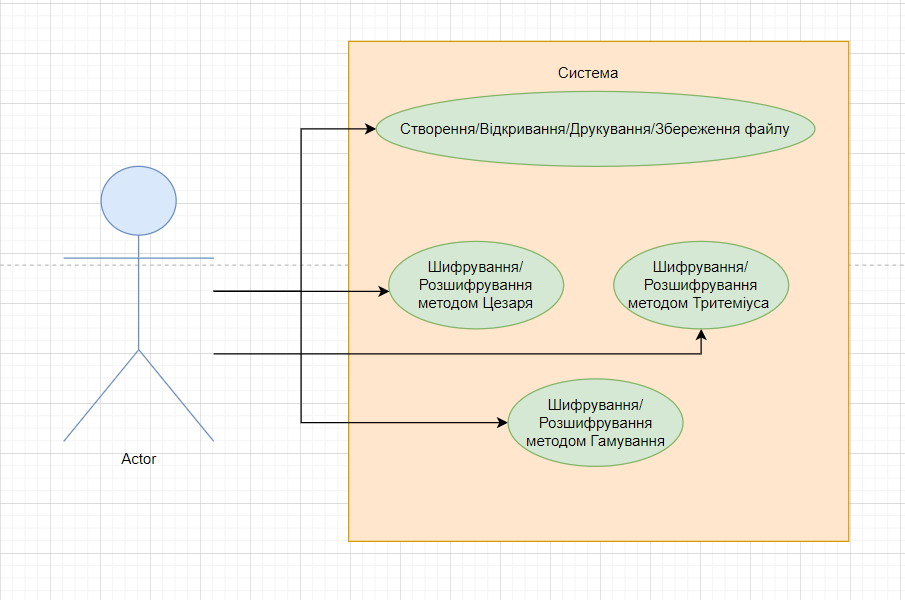
Перевірив: доцент, к.ф.-м.н.  
Тарнавський Ю.А.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

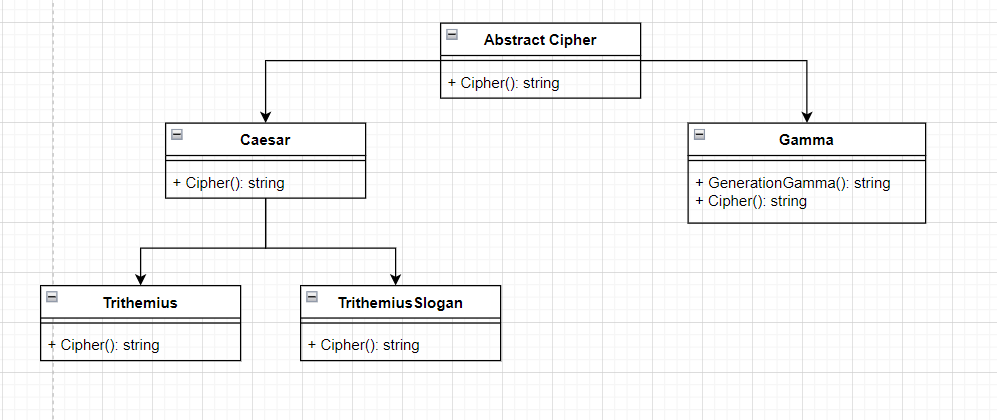
# **Мета роботи**

Розробити криптосистему на основі шифру гамування

# **Діаграма прецедентів**



# **Діаграма класів**



# **Фрагмент коду з реалізацією алгоритму шифрування/розшифрування**

**AbstractCipher**

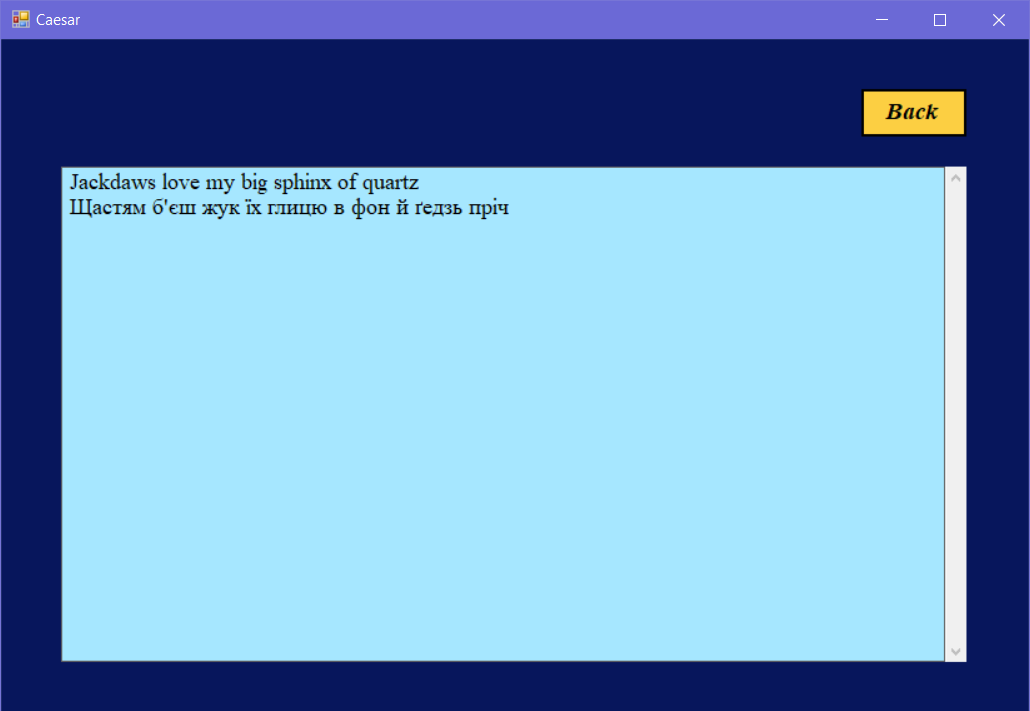
public abstract class AbstractCipher  
**{** protected const int AlphabetSize = 55295**;** // кількість символів в алфавіті Unicode  
   
 public abstract string Cipher(bool variant**,** string[] text**,** string startKey)**;**}

**Gamma**

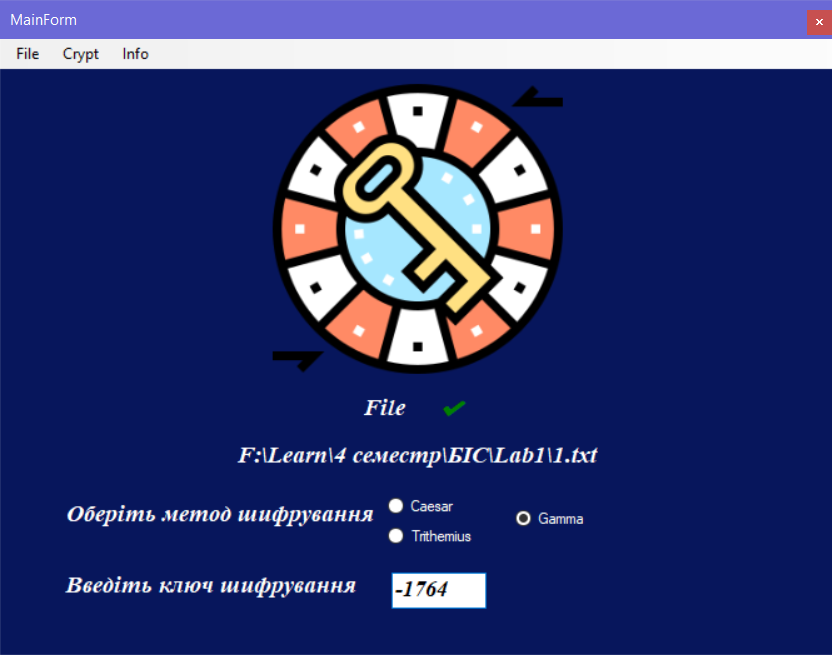
public class Gamma : AbstractCipher  
**{** private string GenerationGamma(string[] text**,** int sead)  
 {  
 var maxLen = text[0].Length**;** for (int i = 1**;** i < text.Length**;** i++)  
 {  
 if (text[i].Length > maxLen)  
 {  
 maxLen = text[i].Length**;** }  
 }  
 var random = new Random(sead)**;** var randomSymbols = Enumerable.*Range*(0**,** maxLen).Select(x => (char)random.Next(1**,** AlphabetSize))**;** return string.*Concat*(randomSymbols)**;** }  
  
 public override string Cipher(bool variant**,** string[] text**,** string startKey)  
 {  
 var cipherText = new StringBuilder()**;** string key = GenerationGamma(text**,** int.*Parse*(startKey))**;** foreach (var lineOfText in text)  
 {  
 for (int i = 0**;** i < lineOfText.Length**;** i++)  
 {  
 int intSymbol = lineOfText[i]**;** int keyCharValue = key[i]**;** int res = intSymbol ^ keyCharValue**;** cipherText.Append((char)res)**;** }  
  
 cipherText.AppendLine()**;** }  
  
 return cipherText.ToString()**;** }  
**}**

# **Скріншоти програми**

Оберемо панграму



Оберемо метод гамування та введемо довільний ключ



Після шифрування виводиться зашифрований текст 

Зберігаємо файл. Для розшифрування вводимо ключ та розшифровуємо. У результаті маємо розшифрований текст



# **Висновки**

На цій лабораторній роботі було ознайомлено з теоретичними відомостями про шифрування методом гамування. Модифіковано програму, розроблену у 2 лабораторній роботі, з графічним інтерфейсом на мові програмування C# з використанням Windows Forms. У програму доповнено новий метод гамування . Виконано тестування роботи шифрування та розшифрування.